BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-203
1 JANUARY 1997

Communications and Information

THE AIR FORCE EMISSION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. Paper publications will be discontinued in December 1996.

This instruction implements the emission security (EMSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes the Air Force EMSEC program to comply with National Security Telecommunications and Information Systems Security Policy 300, *National Policy on Control of Compromising Emanations;* National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000 (C), *TEMPEST Countermeasures for Facilities (U);* NSTISSI 7001 (S), *NONSTOP Countermeasures* (U), and Department of Defense (DoD) Directive 5200.19 (C), *Control of Compromising Emanations (U), 16 May 1995*. It interfaces with Air Force Systems Security Instructions (AFSSI) 4100 (C), *The Communications Security (COMSEC) Program* (will be replaced by AFI 33-201 [S]), 5100, *The Air Force Computer Security (COMPUSEC) Program* and 5102, *Computer Security (COMPUSEC) for Operational* Systems (will be replaced by Air Force Instructions (AFI) 33-202), and AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*. Use of extracts is encouraged. Direct questions and comments on the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA)/SYS, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234, with an information copy to Headquarters United States Air Force (HQ USAF)/SCTW, 1250 Air Force Pentagon, Washington DC 20330-1250. Refer recommended changes and conflicts between this and other publications, on AF Form 847, **Recommendation for Change of Publication**, through channels, to HQ AFCA/XPPD, 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5224. The Glossary of References, Abbreviations, Acronyms, and Terms is at attachment 1.

SUMMARY OF REVISIONS

It aligns with AFPD 33-2 and replaces the Air Force TEMPEST Program with the Air Force EMSEC program. It establishes procedures to control compromising emanations (CE), identifies NONSTOP countermeasures (CM), and prevents HIJACK hazards. It changes the Acceptance of TEMPEST Risk to a temporary waiver, reduces EMSEC inspection requirements, and reflects the reduction in EMSEC testing. It adjusts responsibilities to reflect the realignment of missions within the Air Force.

Supersedes: AFSSI 7000, 2 June 1992.
OPR: HQ AFCA/SYSA (Dwight H. Bohl)

Certified by: HQ USAF/SCXX (Col Brian D. Miller)
Pages: 15/Distribution: F

Please Recycle Printed on Recycled Paper

Section A—The Emission Security Program

1. Introduction. The Air Force EMSEC program has experienced many changes. Although these changes were attempts to meet the variances of a dynamic world, they require security protection measures far beyond the needs of the average user. We now require a more balanced approach to the control of CEs and must include NONSTOP and HIJACK. The prime objective of EMSEC is to identify requirements from the standpoint of Information Protection (IP) risk management principles and provide the appropriate protection at the least possible, or no cost. Key to this program is a partnership between the user and the IP office. Together, they assess the need for EMSEC as part of IP; determine the required CMs; advise commanders of vulnerabilities, threats, and risks; and recommend a practical and feasible course of action to the wing commander.

2. Emission Security Requirements. Air Force organizations and contractors acquiring or using systems to process classified information must apply EMSEC proportional to the threat of exploitation and the potential damage to national security if the classified information is compromised.
2.1. Assess the need for EMSEC for each aspect (control of CEs, NONSTOP, and HIJACK), the inspectable space, and the specific CMs before beginning architectural engineering and facility design, acquiring systems, or beginning engineering and installation.
2.2. Implement or apply required CMs before using systems to process classified information.
2.3. Operate and maintain systems to preserve the integrity of required CMs.
2.4. Processing classified information without complying with the above requirements is a reportable security incident under AFI 31-401, *Managing the Information Security Program,* except as allowed for by waiver in paragraph 10.
2.5. Although EMSEC requirements are lower within the United States, its trust territories and possessions, requirements still exist. EMSEC requirements are higher outside the United States.

3. Emission Security Process. Assess equipment and facilities to determine the need for EMSEC (control of CEs, NONSTOP, and HIJACK); determine which CMs are required; validate the required CMs; implement or apply the required CMs; and periodically reassess EMSEC requirements. The following paragraphs further define this process. (See attachment 2.)

4. The Emission Security Assessment. This determines the need for EMSEC for a system that processes classified information.
4.1. The using Air Force organization determines if the system will process classified information.
4.2. If the system will process classified information, you must contact the local IP office.
4.2.1. The wing IP office makes the EMSEC assessment for wing-level systems and programs.
4.2.2. The major command (MAJCOM) IP office makes the EMSEC assessment for MAJCOM-level programs.
4.2.3. The lead MAJCOM IP office or the Certified TEMPEST Technical Authority (CTTA) makes the EMSEC assessment for Air Force-level programs.
4.2.4. For information that is special category (SPECAT), the SPECAT EMSEC manager or the CTTA makes the EMSEC assessment.

4.3. There are three parts to the assessment: control of CEs, NONSTOP, and HIJACK. Use AFSSI 7010 (S), *The Emission Security Assessment* (U), to make the assessment. Each part has three outcomes: not applicable; no CMs are required; or CMs are required.
4.4. Document the EMSEC assessment on AFCOMSEC Form 7001, **Emission Security Assessment/Emission Security Countermeasures Review**, according to AFSSI 7010 (S).

5. The Emission Security Countermeasures Review . There are three reviews required to identify CM requirements; control of CEs, NONSTOP, and HIJACK. Use Air Force Systems Security Memorandum (AFSSM) 7011, *The Emission Security Countermeasures Review*, to make each review.
5.1. The Control of Compromising Emanations Countermeasures Review. This review uses the inspectable space, the equipment TEMPEST characteristics, and the facility characteristics to determine the required CMs.
5.2. The NONSTOP Countermeasures Review. This review uses distance, the equipment TEMPEST characteristics, and the facility characteristics to determine the required CMs.
5.3. The HIJACK Countermeasures Review. This review uses type of information processed to determine the required CMs.
5.4. Documenting The Countermeasures Review. Whenever possible, document all CM reviews on the same AFCOMSEC Form 7001 as used for the EMSEC assessment.

6. Validation Requirements. Validate CMs reviews according to AFSSI 7010.

7. Applying Countermeasures. The user implements the required CMs identified by the CMs reviews. The wing IP office completes an EMSEC inspection, when required (see paragraph 9), to make sure of compliance and effectiveness.

8. Reassessing Requirements. Reassess the EMSEC requirements during a reinspection, when required by a computer security risk analysis, the threat changes, or the classification level of the information changes.

9. Emission Security Inspections. The CMs review is the basis for the EMSEC inspection. The user must correct deficiencies discovered by an EMSEC inspection or request a temporary or permanent waiver before processing classified information. The purpose of the initial inspection is to make sure the required CMs are effectively implemented or applied before processing classified information. The purpose of a reinspection is to make sure the required CMs are still effective.
9.1. Facilities Requiring the Control of Compromising Emanations. Make an initial inspection and annual reinspection of all facilities requiring CMs where:
9.1.1. TOP SECRET information is processed.
9.1.2. SECRET information is processed in facilities located outside the United States, its trust territories and possessions.
9.2. Facilities Requiring NONSTOP Countermeasures. Make an initial inspection of all facilities requiring NONSTOP CMs. Reinspect every 3 years or when the threat or classification level of the information changes.
9.3. Facilities Requiring HIJACK Countermeasures. Make an initial inspection of all facilities requiring HIJACK CMs. Reinspect every 3 years or when the threat or classification level of the information changes.

10. Waivers. There are two kinds of waivers: temporary and permanent.
10.1. AFCOMSEC Form 3331, Request for Waiver From Information Protection Criteria. Use this form to document and request either a temporary (see attachment 3) or permanent waiver (see attachment 4). Attach a copy of the assessment and CMs review.
10.2. Temporary Waiver. A temporary waiver allows the processing of classified information when the user is not able to implement or apply all required CMs. A temporary waiver is valid for 1 year to allow the user to accomplish the mission while they implement or apply all required CMs.
10.2.1. Conditions. The following conditions must exist before processing a temporary waiver:
10.2.1.1. All required CMs were not installed or applied during installation.
10.2.1.2. Operation is required for mission accomplishment.
10.2.1.3. You cannot install all required CMs before system turn-on.
10.2.2. Processing a Temporary Waiver. The user originates a temporary waiver, then sends it to the wing IP office for coordination, and approval or disapproval by the appropriate authority.
10.2.2.1. The Control of Compromising Emanations.
10.2.2.1.1. For collateral TOP SECRET information, the approval authority for the temporary waiver is the wing commander or designated user representative (not the wing IP office).
10.2.2.1.2. For collateral SECRET and below information, the approval authority is the designated approving authority (DAA).
10.2.2.1.3. For SPECAT information, process the temporary waiver through the SPECAT EMSEC manager to the DAA.

10.2.2.1.4. For Global Command and Control System (GCCS) information, process the temporary waiver through the MAJCOM IP office to the GCCS DAA.
10.2.2.2. NONSTOP and HIJACK. Note: The terms NONSTOP and HIJACK have classified definitions; see AFMAN 33-272.
10.2.2.2.1. For collateral information, the approval authority is the Air Force CTTA.
10.2.2.2.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC manager to the CTTA.
10.2.2.2.3. For GCCS information, process the temporary waiver through the MAJCOM IP office to the GCCS CTTA.
10.2.3. Temporary Waiver Renewals. A temporary waiver is renewable for 1 year only if the user is making an active effort to correct the problem; otherwise do not renew it. Process a renewal according to paragraph 10.2.2 before the current temporary waiver expires. Only two renewals are permitted.
10.2.4. Temporary Waiver Cancellations. Cancel the temporary waiver after applying the required CMs (see attachment 3 for instructions).
10.2.5. Temporary Waiver Copies. Forward a copy of all temporary waivers, including renewals and cancellations, to the MAJCOM IP office or SPECAT EMSEC Manager and HQ AFCA/SYS.
10.3. Permanent Waiver. The CTTA may waive a specific CM. Such things as an extremely low volume of classified information, a low level of classification, disproportionate costs, impossible to do, or other conditions that make the application of the CM seem inappropriate to the IP office are the basis for a waiver. The CTTA approves permanent waivers (see attachment 4 for instructions). Permanent waivers have no expiration date. Process requests as follows:
10.3.1. The user initiates the request and forwards it to the wing IP office for review.
10.3.2. The wing IP office reviews the request for validity and if valid, sends it to the MAJCOM IP office or SPECAT EMSEC manager for review.
10.3.3. The MAJCOM IP office or SPECAT EMSEC manager reviews the request and if valid, forwards it, along with appropriate supportive comments, to HQ AFCA/SYS for review and approval or disapproval by a CTTA.

Section B—Responsibilities

11. Responsibilities and Authority. This instruction establishes the following responsibilities and authorities.
11.1. HQ USAF/SCTW. Responsible for the EMSEC program according to AFPD 33-2. It establishes Air Force EMSEC policy and doctrine, and coordinates with the other
military departments and government agencies to eliminate duplication and to exchange technical data.
11.2. HQ USAF, Deputy Chief of Staff, Civil Engineering (HQ USAF/CE). The Air Force focal point for design and construction of facilities containing radio frequency interference (RFI) and electromagnetic interference (EMI) shielding.
11.2.1. Air Force Civil Engineering Support Agency (AFCESA/ENE) is the OPR for guidance, information, and requirements for design and construction of facilities containing RFI and EMI shielding.
11.3. Headquarters Air Force Communications Agency (HQ AFCA):
11.3.1. Manages the Air Force EMSEC Program.
11.3.2. Is assigned CTTA responsibility (paragraph 10).
11.3.3. Distributes guidance on the domestic and foreign technical threat environment as provided by the National Security Agency (NSA).
11.3.4. Tasks all Air Force EMSEC testing.
11.3.5. Advises Headquarters Air Education and Training Command (HQ AETC) on EMSEC curriculum.
11.3.6. Provides Air Force EMSEC requirements and guidance for Air Force systems.
11.3.7. Reviews, approves or disapproves, the installation plans that have EMSEC requirements when the installation is contracted.
11.3.8. Provides Air Force organizations disposition instructions for TEMPEST-certified and formerly TEMPEST-certified equipment.
11.4. Headquarters Air Intelligence Agency (HQ AIA). As the technical consultant on shielding materials and construction techniques for Air Force real property shielding for the control of CEs:
11.4.1. Assists AFCESA/ENE:
11.4.1.1. Develops design and construction standards for shielding in facilities.
11.4.1.2. Reviews designs, specifications, and construction drawings for shielding in facilities.
11.4.1.3. Resolves construction problems due to shielding in facilities through site visits.
11.4.1.4. Participates in final acceptance inspections of shielding in facilities.
11.4.2. Assists Headquarters Air Force Materiel Command (HQ AFMC), in standardization of RFI and EMI filters for shielding in facilities.
11.5. Air Force Information Warfare Center (AFIWC):
11.5.1. Provides a quick reaction capability to support emergency testing of facilities and NONSTOP and HIJACK testing.

11.5.2. Provides a capability for limited testing of high-value Air Force systems such as special air mission aircraft and strategic systems (i.e., F-117, B-2, black, or special access required programs).
11.5.3. Secures a fee-for-service contracting vehicle for routine and standard EMSEC testing support.
11.5.4. Manages the Air Force EMSEC testing program to include contract monitoring and oversight duties.
11.5.5. Provides technical oversight of all contracted Air Force EMSEC tests.
11.5.6. Interacts with the US Government TEMPEST technical community.
11.5.7. Serves as the Air Force technical consultant for emerging EMSEC issues.
11.5.8. Provides a limited testing and evaluation capability for Air Force automated information systems (AIS) in a laboratory environment for zoning and profiling.
11.6. MAJCOMs: (Includes those Field Operating Agencies [FOA] and Direct Reporting Units [DRU] who manage their own EMSEC program [see paragraph 11.8].)
11.6.1. Establish an EMSEC program in the MAJCOM IP office. Include those Air National Guard and United States Air Force Reserve units gained by the MAJCOM on activation.
11.6.2. Include EMSEC requirements identified by the MAJCOM IP office in requests for proposal, specifications, statements of work, operational requirements documents (ORD), program management directives, and contracts when planning and programming for a procurement requirement for systems (includes facilities and individual pieces of equipment) that will process classified information. This includes systems under development and those embedded in weapons systems. Review mission need statements (MNS) and equipment specifications for EMSEC considerations and criteria.
11.6.3. Include EMSEC requirements when preparing the communications security appendix to the communications annex of operations plans according to AFI 10-401, *Operation Plan and Concept Plan Development and Implementation*.
11.6.4. Implement and maintain required CMs for systems that process classified information.
11.6.5. Notify wing and regional civil engineers of any unique construction needed to support programs that process classified information.
11.6.6. Make sure inspection of all facilities which have EMSEC requirements (paragraph 9).
11.7. MAJCOM IP Office:
11.7.1. Is the OPR for the MAJCOM EMSEC program.
11.7.2. Requests emission profiles from HQ AFCA/SYS to make CMs reviews and EMSEC inspections.
11.7.3. Provides EMSEC guidance and assistance to the command staff and subordinate wing IP offices.
11.7.4. When requested, assists wing IP offices by making EMSEC assessments, CMs reviews, and EMSEC inspections.
11.7.5. Reviews and approves EMSEC requirements for contractor facilities for MAJCOM contracts.
11.7.6. Coordinates with the MAJCOM formal training office to establish an EMSEC training priority system so units with the greatest need for formal EMSEC training get the highest priority.
11.7.7. Assists and provides guidance to the MAJCOM civil engineer for correction of real property EMSEC deficiencies.
11.7.8. Reviews MAJCOM programming and requirements documents that call for the processing of classified information.
11.7.9. For projects that involve more than one wing within the MAJCOM or for MAJCOM programs:
11.7.9.1. Reviews all project support agreements (PSA) changes, and project packages for facilities that will process classified information.
11.7.9.2. Coordinates with affected wings for the EMSEC assessments and CMs reviews.
11.7.9.3. Advises command program managers of required CMs.
11.8. Host Air Force Wings:
11.8.1. Establish an EMSEC program in the host wing IP office. This office addresses all EMSEC requirements on the base, including those of tenant units (FOAs, DRUs, and other MAJCOM units), unless other formal agreements are made.
11.8.1.1. When justified and approved, an FOA or DRU may establish its own EMSEC program. Send requests for approval with justification to HQ AFCA/SYS. If approved, establish a MAJCOM IP office and comply with paragraphs 11.6, 11.7, 11.8, and 11.9.
11.8.1.2. An IP office may support non-Air Force units if their own service does not, and the unit requests support.
11.8.2. Include a wing IP office representative in planning meetings for new equipment acquisition, installation, or reconfiguration of existing facilities that process classified information.
11.8.3. Assist the wing IP office to determine EMSEC requirements and, when required, cost estimates of required CMs during initial meetings for new facility construction or upgrade projects.
11.9. Wing IP Office:
11.9.1. Manages the wing EMSEC program.
11.9.2. Makes EMSEC assessments of all systems that process classified information on the base, including those of tenant organizations, unless other formal agreements are made. Makes CMs reviews when required. Maintains a file of all current EMSEC assessments and CMs reviews. Forwards a copy of all CMs reviews according to AFSSM 7011, *The Emission Security Countermeasures Review*.

11.9.3. Requests emission profiles from the MAJCOM IP office or SPECAT EMSEC manager for equipment and systems to make CMs reviews and EMSEC inspections.
11.9.4. Conducts and documents required initial and annual EMSEC inspections. Files the latest EMSEC inspection with the corresponding current CMs review.
11.9.5. Advises commanders, managers, supervisors, or users of CMs required to adequately protect classified information (the CMs review) and what deficiencies exist for their systems (the EMSEC inspection).
11.9.6. Maintains a file of all active temporary and permanent waivers.
11.9.7. Makes sure current required Air Force EMSEC guidance and information are given wide dissemination.
11.9.8. Provides HQ 38 Engineering Installation Wing (HQ 38EIW), Tinker OK 73145-2700, with CM requirements for C4 systems before engineering and installation begins.
11.9.9. Assists the wing civil engineer in planning new facilities, or reconfiguring existing facilities, that process classified information. Advises the wing civil engineer of any CM requirements for new construction or upgrade projects.
11.9.10. Reviews and approves required CMs for contractor facilities supporting wing contracts.
11.9.11. Helps the contracting officer obtain standards necessary for contractual compliance with EMSEC requirements.
11.9.12. Reviews all PSAs, PSA changes, and project packages for facilities that will process classified information, to make sure applicable EMSEC requirements are included.
11.9.13. Assists users with the technical aspects of applying CMs.
11.9.14. Coordinates on AF Form 1261, **Command, Control, Communications and Computer Systems Acceptance Certificate**, before the user processes any classified information.
11.10. HQ AETC. In addition to the responsibilities in paragraph 11.6, HQ AETC:
11.10.1. Trains or makes sure training is provided to installers, operators, and maintenance technicians of systems that process classified information.
11.10.2. Conducts EMSEC training according to AFI 36-2201, *Developing, Managing, and Conducting Training*.
11.10.3. Works with HQ AFCA/SYS to make sure EMSEC portions of curriculums are current and meet Air Force needs.
11.11. HQ AFMC. In addition to the responsibilities in paragraph 11.6, HQ AFMC:
11.11.1. Makes sure EMSEC-related configuration control information is available to the operations, maintenance, and logistics-support organizations to maintain the integrity of CMs during a system's life cycle.
11.11.2. Issues time-compliance technical orders and modification kits for equipment and systems that are under its inventory management control and are scheduled for modification.
11.11.3. Establishes configuration control procedures to make sure there is continuity and integrity of CMs for equipment and systems that process classified information under its inventory management
11.11.4. Makes sure technical analyses, cost estimates, and modification proposals for systems that process classified information consider TEMPEST design and installation requirements.
11.11.5. Conducts a studies and analysis program that will result in research, development, test, and evaluation of TEMPEST test equipment and techniques. Coordinates TEMPEST information exchange with AFIWC/EAC.
11.11.6. Assists AFCESA/ENE and HQ AIA in standardization of RFI and EMI filters for shielding in facilities.
11.11.7. Uses the MAJCOM and wing IP offices at their engineering and development centers to make EMSEC assessments and CMs reviews for its program managers.
11.11.8. Installs equipment and systems according to EMSEC standards.
11.11.9. Makes sure installation standards retain or enhance EMSEC integrity.
11.11.10. Coordinates exchange of engineering and installation EMSEC information with HQ AFCA/SYS.
11.11.11. Performs shielding-effectiveness testing when requested.
11.11.12. Provides, when requested, cost estimates for the installation of required CMs. Estimates do not include costs based on good engineering practices as EMSEC CMs costs. Cost estimates reflect only the delta increase of CM costs.
11.12. Program Managers. Responsible for early coordination with MAJCOM IP offices, SPECAT EMSEC managers, and wing IP offices to:
11.12.1. Make sure EMSEC requirements are included in MNSs, ORDs, and so forth.
11.12.2. Establish EMSEC requirements at locations where the system will be used.
11.13. Air Force C4 Systems Users:
11.13.1. Contact the wing IP office (FOA or DRU IP office for those FOAs and DRUs managing their own EMSEC program) for assistance as soon as you determine you need to process classified information.
11.13.2. Request the wing IP office make an EMSEC assessment to identify the need for EMSEC at the earliest date possible.
11.13.3. Make sure you implement required CMs.
11.13.4. Request the wing IP office perform an initial EMSEC inspection, after installation, but before operation, if required (paragraph 9).
11.13.5. Correct all deficiencies identified by an EMSEC inspection and request a reinspection.

11.13.6. Maintain CMs to as-applied or as-installed conditions.
11.13.7. Initiate requests for temporary and permanent waivers (paragraph 10) and EMSEC tests (AFSSM 7011), when needed.
11.14. Special Category Facilities. Facilities that process SPECAT classified information are administered outside the normal chain of command and require special EMSEC support. Air Force policy applies to SPECAT facilities funded by the Air Force.
11.14.1. SPECAT Program Managers:
11.14.1.1. Defense Intelligence Agency (DIA/DAC-2A) is the SPECAT program manager for all DIA-accredited sensitive compartmental information facilities (SCIF).
11.14.1.2. NSA is the SPECAT Program manager for all NSA accredited SCIFs.
11.14.1.3. SAF/AQL-PJ is the SPECAT program manager for special access programs.
11.14.2. SPECAT EMSEC Managers. SPECAT EMSEC managers have the responsibilities of the:
11.14.2.1. MAJCOM IP office as defined in paragraph 11.7.
11.14.2.2. Wing IP office as defined in paragraph 11.9 at bases where the local wing IP office is not available or used.
11.14.3. Identify SPECAT EMSEC Managers. Identify the SPECAT EMSEC manager to HQ AFCA/SYS. SPECAT EMSEC manager offices are:
11.14.3.1. HQ DIA/DAC-2A for Special Compartmented Information Facilities.
11.14.3.2. HQ AIA/SOXS for Air Force SCIFs.
11.14.3.3. SAF/AQL-PJ for Special Access Programs.
11.14.3.4. Identified by program directive or special order.
11.14.4. Wing IP Office Support. For EMSEC, wing IP offices provide two important services, when requested:
11.14.4.1. Make the EMSEC assessment and CMs review of the facility using AFSSI 7010 (S) and AFSSM 7011.
11.14.4.2. Make the initial and annual EMSEC inspections.

Section C—Qualifications and Classification

12. Certified TEMPEST Technical Authority. A CTTA is an experienced, technically-qualified government employee who meets established certification requirements according to NSTISSC-approved criteria and has been appointed by HQ USAF/SCTW to fulfill CTTA responsibilities. A CTTA conducts, validates, or reviews CMs reviews to determine compliance with applicable national, DoD, and Air Force policy and instructions. A CTTA must meet the following requirements:
12.1. Complete 3 continuous years of TEMPEST technical experience, including at least 1 year of experience evaluating vulnerabilities of operational facilities and recommending CMs.
12.2. Complete mandatory training on the technical threat.
12.3. Complete technical training identified by the national manager for National Security Telecommunications, and AIS Security. HQ USAF/SCTW may waive technical training requirements.

13. Classification Guidance. AFMAN 33-272 (S), *Classifying Communications Security, Tempest, and C4 Systems Security Research and Development Information* (U), is the classification guide for EMSEC matters.

14. Forms Prescribed. This instruction prescribes:
14.1. AFCOMSEC Form 3331, **Request for Waiver From Information Protection Criteria.**
14.2. AFCOMSEC Form 7001, **Emission Security Assessment/Emission Security Countermeasures Review.**

JOHN S. FAIRFIELD, Lt General, USAF
DCS/Communications and Information

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

Executive Order 12958, *Classified National Security Information*
DoD Directive 5200.19 (C), *Control of Compromising Emanations* (U), 16 May 1995
NSTISSI 7000 (C), *Tempest Countermeasures for Facilities (U)*
NSTISSI 7001 (S), *NONSTOP Countermeasures (U)*
AFPD 33-2, *C4 Systems Security*
AFI 10-401, *Operation Plan and Concept Plan Development and Implementation*
AFI 31-401, *Managing the Information Security Program*
AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*
AFI 36-2201, *Developing, Managing, and Conducting Training*
AFMAN 33-272 (S), *Classifying Communications Security, Tempest, and C4 Systems Security Research and Development Information* (U)
AFSSI 4100 (C), *The Communications Security (COMSEC) Program* (will be replaced by AFI 33-201 [S]),
AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program* (will be replaced by AFI 33-202)
AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems* (will be replaced by AFI 33-202)
AFSSI 7010 (S), *The Emission Security Assessment (U)*
AFSSM 7011, *The Emission Security Countermeasures Review*

Abbreviations and Acronyms

AETC−Air Education and Training Command
AFCA−Air Force Communications Agency
AFCESA−Air Force Civil Engineering Support Agency
AFI−Air Force Instruction
AFIWC−Air Intelligence Agency Air Force Information Warfare Center Communications-Computer System
AFMAN−Air Force Manual
AFMC−Air Force Material Command
AFPD−Air Force Policy Directive
AFSSI−Air Force Systems Security Instruction
AFSSM−Air Force Systems Security Memorandum
AIS−Automated Information System
C4−Command, Control, Communications, and Computers
CE−Compromising Emanations
CM−Countermeasure
CTTA−Certified TEMPEST Technical Authority
DAA−Designated Approving Authority
DIA−Defense Intelligence Agency
DoD−Department of Defense
DRU−Direct Reporting Unit
EIW−Engineering Installation Wing
EMI−Electromagnetic Interference
EMSEC−Emission Security
EO−Executive Order
FOA−Field Operating Agency
GCCS−Global Command and Control System
HQ AIA−Headquarters Air Intelligence Agency
IP−Information Protection
JP−Joint Publication
MAJCOM−Major Command
MNS−Mission Need Statement
NSA−National Security Agency
NSI−National Security Information
NSTISSAM−National Security Telecommunications and Information Systems Security Action Memorandum
NSTISSC−National Security Telecommunications and Information Systems Security Committee

NSTISSI−National Security Telecommunications and Information Systems Security Instruction
OPR−Office of Primary Responsibility
ORD−Operational Requirements Document
PSA−Project Support Agreement
RFI−Radio Frequency Interference
SCIF−Sensitive Compartmented Information Facility
SPECAT−Special Category
USAF−United States Air Force

Terms

Certified TEMPEST Technical Authority —An experienced, technically qualified government employee who has met established certification requirements according to NSTISSC-approved criteria and has been appointed by a United States Government department or agency to fulfill CTTA responsibilities.
Collateral Information —All NSI classified information under the provisions of an executive order (EO), for which special community systems of compartments (for example, sensitive compartmented information) are not formally established.
Compromising Emanation —Unintentional signal that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information-processing equipment.
Countermeasures —A form of military science which, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02) Any action, device, procedure, technique, or other means that reduces the vulnerability of an AIS.
Countermeasures Review —A technical evaluation of a facility to identify the inspectable space, the required CMs, and the most cost effective way to apply required CMs.
Emanation —Unintended signals or noise appearing external to an equipment.
Emission Security —The protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of CEs from crypto-equipment, information systems, and telecommunications systems.
Emission Security Assessment —An evaluation of a facility to determine the need for EMSEC.
Emission Security Countermeasures Review —A review of a facility to determine needed CMs.
Equipment Radiation TEMPEST Zone —A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of CEs is considered possible.
Facility —(1) A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (JP 1-02) (2) A physically definable area which contains classified information-processing equipment.
Hazard —A measure of both the existence and the compromising nature of an emanation. Hazards exist if and only if CEs are detectable beyond the inspectable space.
HIJACK —The definition of HIJACK is classified.
Inspectable Space —The three-dimensional space surrounding equipment that processes classified or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify or remove a potential TEMPEST exploitation exists.
National Security Information —Information that has been determined, pursuant to EO 12958, or any predecessor order, to require protection against unauthorized disclosure, and is so designated.
NONSTOP —The definition of NONSTOP is classified.
RED and BLACK Concept —Separation of electrical and electronic circuits, components, equipment, and systems which handle classified plain text (RED) information in electrical signal form from those which handle unclassified (BLACK) information in the same form.
Service Cryptologic Element —A term used to designate separately or together those elements of the United States Army, United States Navy, and United States Air Force which perform cryptologic functions.
Special Category Information —The definition of SPECAT is classified. (See AFSSI 7010 (S))
TEMPEST —An unclassified term referring to technical investigations for CEs from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security.
TEMPEST-Certified Equipment —Systems or equipment which were certified within the requirements of the effective edition of NSTISSAM TEMPEST/1-92, Level I, or TEMPEST specifications as determined by the department or agency concerned.

THE EMISSION SECURITY FLOW CHART

This is a flow chart of the EMSEC process.

Figure A2.1. The Emission Security Flowchart.

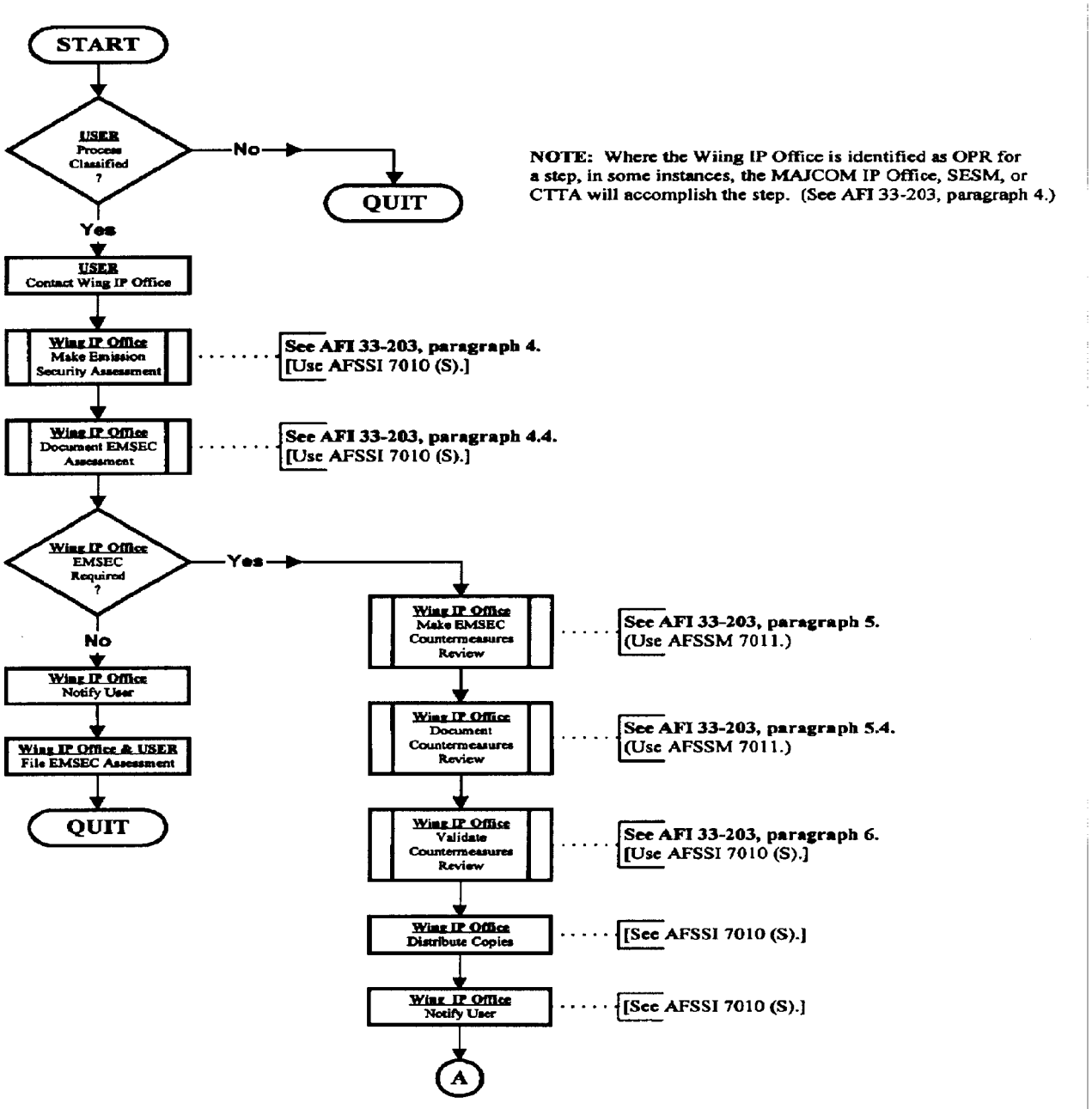
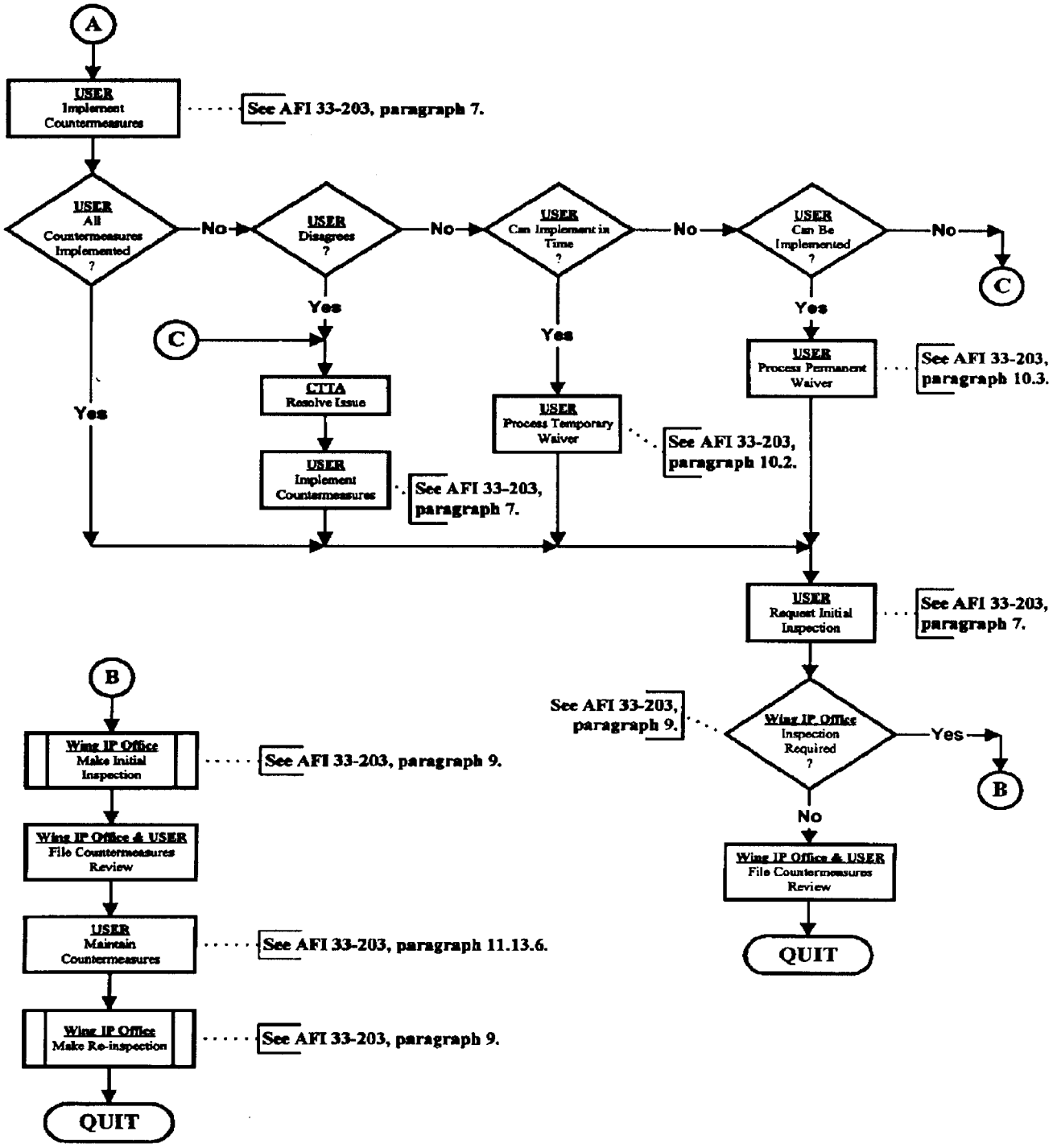


Figure A2.1. Continued.



PROCEDURES FOR COMPLETING AFCOMSEC FORM 3331 FOR A TEMPORARY WAIVER

A3.1. Temporary Waiver. This attachment provides guidance for completing AFCOMSEC Form 3331 for a temporary waiver. Due to the limited space on the form, attach additional information as required.

A3.2. Filling out the form for Collateral TOP SECRET and below.

A3.2.1. Block 1: The wing IP office numbers the initial temporary waiver using the following format: requesting unit-last two digits of year-minimum two digit temporary waiver number with a "T." Use the original temporary waiver number for renewals.

Examples: 1776ABW-95-01T, 1925CS-95-104T.

A3.2.2. Block 2: Not to exceed 1 year from the date of approval block 30.

A3.2.3. TO: Either a senior manager in the user's chain to the wing commander or the wing IP office; use organization and office symbol.

A3.2.4. FROM: The requester's organization and office symbol.

A3.2.5. Block 3: Check "temporary" and either "initial," "renewal," or "cancellation."

NOTE: For cancellations, skip blocks 4 through 6 and 8 through 18.

A3.2.6. Block 4: Base, building, room number, organization, office symbol, and title.

A3.2.7. Block 5: List the specific CMs not met.

A3.2.8. Block 6: State the problem briefly. If the approving authority will need more information than will fit in the block to fully understand the problem, use plain bond paper and attach the continued discussion.

A3.2.9. Block 7: Briefly explain your justification for processing classified information without meeting all the required CMs. For example, what is the mission impact of not processing? Why can't you apply the CMs before system turn-on? Attach a copy of the EMSEC CMs review, AFCOMSEC Form 7001.

A3.2.9.1. For renewals: The first entry in block 7 must be, "The initial temporary waiver approved date is .... ."

A3.2.9.2. For cancellations: Explain the cancellation for example, "CMs applied" or "equipment no longer used to process classified information."

A3.2.10. Block 8:

A3.2.10.1. Initial: List interim procedures to lessen the risk while the temporary waiver is in effect.

A3.2.10.2. Renewal: Indicate the corrective actions you have taken to date.

A3.2.11. Block 9:

A3.2.11.1. Initial: State the action that will correct the deficiency. State the date corrective measures will start. State the completion date for corrective measures.

A3.2.11.2. Renewal: State what corrective actions remain. State the date remaining corrective measures will start. State the completion date for remaining corrective measures.

A3.2.12. Blocks 10 and 11: Self explanatory.

A3.2.13. Blocks 12: As necessary within the requester's organization.

A3.2.14. Blocks 13 through 15: Self explanatory.

A3.2.15. Reviewing official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IP Office is mandatory. It is the last review before forwarding the request to the wing commander. No more than two reviews are allowed.

A3.2.16. First reviewing official.

A3.2.16.1. TO: Either the wing IP office, the DAA (permitted for SECRET and below), or the wing commander (required for TOP SECRET).

A3.2.16.2. FROM: This reviewer (organization and office symbol); either a manager in the user's chain or the wing IP office.

A3.2.16.3. Block 16: As necessary within the reviewer's organization.

A3.2.16.4. Block 17: Self explanatory.

A3.2.16.5. Block 18: Mark the "approval" or "disapproval" block.

A3.2.16.6. Blocks 19 through 21: Self explanatory.

A3.2.17. Final reviewing official.

A3.2.17.1. TO: Either the DAA (permitted for SECRET and below) or the wing commander (required for TOP SECRET).

A3.2.17.2. FROM: The wing IP office (organization and office symbol).

A3.2.17.3. Block 16 or 22: As necessary within the wing IP office.

A3.2.17.4. Block 17 or 23: Self explanatory.

A3.2.17.5. Block 18 or 24: Mark the "approval" or "disapproval" block.

A3.2.17.6. Blocks 19 through 21 or 25 through 27: Self explanatory.
A3.2.18. Approval authority: Use this area to approve the temporary waiver.
A3.2.18.1. TO: The requester; organization and office symbol.
A3.2.18.2. FROM: The DAA (SECRET and below) or the wing commander (required for TOP SECRET).
A3.2.18.3. Block 28: As necessary.
A3.2.18.4. Block 29: Mark the “approved” or “disapproved” or “returned for further action” block.
A3.2.18.5. Block 30: The date this form is signed is the date of approval.
A3.2.18.6. Blocks 31 and 32: Self explanatory.
A3.2.19. Block 33: Place “classified by” and “declassify on” in the bottom right corner of this block by the originator.

A3.3. SPECAT.
A3.3.1. Complete all of paragraphs A3.2.1 through A3.2.14, and A3.2.19.
A3.3.2. In the first TO: block after block 2, add the base to the organization and office symbol.
A3.3.3. Reviewing official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IP office and the SPECAT EMSEC manager is mandatory and is the last review before forwarding the request to the approving authority. If you need reviews, in addition to the wing IP office and SPECAT EMSEC manager, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.
A3.3.4. Reviewing official other than the wing IP office. Any manager in the user’s chain**.**
A3.3.4.1. TO: The next level for review or the wing IP office (organization, office symbol, and base).
A3.3.4.2. FROM: This reviewer (organization, office symbol, and base).
A3.3.4.3. Block 16: As necessary within the reviewer’s organization.
A3.3.4.4. Block 17: Self explanatory.
A3.3.4.5. Block 18: Mark the “approval” or “disapproval” block.
A3.3.4.6. Blocks 19 through 21: Self explanatory.
A3.3.5. The wing IP office’s review.
A3.3.5.1. TO: The SPECAT EMSEC manager (organization, office symbol, and base).
A3.3.5.2. FROM: The wing IP office (organization, office symbol, and base).
A3.3.5.3. Block 16: As necessary within the wing IP office.
A3.3.5.4. Block 17: Self explanatory.
A3.3.5.5. Block 18: Mark the “approval” or “disapproval” block.
A3.3.5.6. Blocks 19 through 21: Self explanatory.
A3.3.6. The SPECAT EMSEC manager’s review.
A3.3.6.1. TO: The SPECAT information DAA (organization, office symbol, and base).
A3.3.6.2. FROM: The SPECAT EMSEC manager (organization and office symbol).
A3.3.6.3. Block 16: As necessary within the SPECAT EMSEC manager’s office.
A3.3.6.4. Block 17: Self explanatory.
A3.3.6.5. Block 18: Mark the “approval” or “disapproval” block.
A3.3.6.6. Blocks 19 through 21: Self explanatory.
A3.3.7. Approval authority: Use this area to approve the temporary waiver.
A3.3.7.1. TO: The requester; organization, office symbol, and base.
A3.3.7.2. FROM: The SPECAT information DAA (organization, office symbol, and base).
A3.3.18.3. Block 28: As necessary.
A3.3.18.4. Block 29: Mark the “approved” or “disapproved” or “returned for further action” block.
A3.3.18.5. Block 30: The date this form is signed is the date of approval.
A3.3.18.6. Blocks 31 and 32: Self explanatory.

PROCEDURES FOR COMPLETING AFCOMSEC FORM 3331 FOR A PERMANENT WAIVER

A4.1. Permanent Waiver. This attachment provides guidance for completing the AFCOMSEC Form 3331 for a permanent waiver. Due to the limited space on the form attach additional information as required.

A4.2. Filling out the form for Collateral TOP SECRET and below.

A4.2.1. Block 1: The wing IP office numbers the initial permanent waiver using the following format: requesting unit-last two digits of year-minimum two digit permanent waiver number with a "P." Use the original temporary waiver number for renewals.

Examples: 1776ABW-95-01P, 1925CS-95-104P.

A4.2.2. Block 2: Enter "no expiration date."

A4.2.3. TO: Either a senior manager in the user's chain to the wing commander or the wing IP office; use organization and office symbol.

A4.2.4. FROM: The requester's organization and office symbol.

A4.2.5. Block 3: Check "permanent."

A4.2.6. Block 4: Base, building, room number, organization, office symbol, and title.

A4.2.7. Block 5: List the specific CM not met; one CM to a request for waiver.

A4.2.8. Block 6: State the problem briefly. If the CTTA will need more information to fully understand the problem, use an attachment and explain thoroughly.

A4.2.9. Block 7: Briefly explain your justification for processing classified information without applying the required CM. For example, why can't the required CM be applied? Attach a copy of the CMs review, AFCOMSEC Form 7001.

A4.2.10. Block 8: List procedures to lessen the risk while the permanent waiver is in effect.

A4.2.11. Blocks 9 through 11: Leave blank.

A4.2.12. Blocks 12: As necessary within the requester's organization.

A4.2.13. Blocks 13 through 15: Self explanatory.

A4.2.14. Reviewing official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing and MAJCOM IP offices is mandatory. It is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing IP Office and SPECAT EMSEC manager, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.

A4.2.15. Reviewing official other than the wing IP office. Any manager in the user's chain.

A4.2.15.1. TO: The next level for review or the wing IP office (organization, office symbol, and base).

A4.2.15.2. FROM: This reviewer (organization, office symbol, and base).

A4.2.15.3. Block 16: As necessary within the reviewer's organization.

A4.2.15.4. Block 17: Self explanatory.

A4.2.15.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.15.6. Blocks 19 through 21: Self explanatory.

A4.2.16. The wing IP office's review.

A4.2.16.1. TO: The MAJCOM IP office (organization, office symbol, and base).

A4.2.16.2. FROM: The wing IP office (organization, office symbol, and base).

A4.2.16.3. Block 16: As necessary within the wing IP office.

A4.2.16.4. Block 17: Self explanatory.

A4.2.16.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.16.6. Blocks 19 through 21: Self explanatory.

A4.2.17. The MAJCOM IP office's review.

A4.2.17.1. TO: The CTTA (organization, office symbol, and base).

A4.2.17.2. FROM: The MAJCOM IP office (organization and office symbol).

A4.2.17.3. Block 16: As necessary within the MAJCOM IP office's office.

A4.2.17.4. Block 17: Self explanatory.

A4.2.17.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.17.6. Blocks 19 through 21: Self explanatory.

A4.2.18. Approval authority: The CTTA uses this area to approve the waiver request.

A4.2.18.1. TO: The requester; organization and office symbol.

A4.2.18.2. FROM: CTTA, HQ AFCA/SYS.

A4.2.18.3. Block 28: As necessary.

A4.2.18.4. Block 29: Mark the "approved" or "disapproved" or "returned for further action" block.

A4.2.18.5. Block 30: The date this form is signed is the date of approval.
A4.2.18.6. Blocks 31 and 32: Self explanatory.
A4.2.19. Block 33: Place “classified by” and “declassify on” in the bottom right corner of this block by the originator.

A4.3. SPECAT.
A4.3.1. Complete all of paragraphs A4.2.1 through A4.2.14, and A4.2.19.
A4.3.2. In the first TO*:* block after block 2, add the base to the organization and office symbol.
A4.3.3. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IP office and the SPECAT EMSEC manager is mandatory and is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing IP office and SPECAT EMSEC manager, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.
A4.3.4. Reviewing official other than the wing IP office. Any manager in the user’s chain**.**
A4.3.4.1. TO: The next level for review or the wing IP office (organization, office symbol, and base).
A4.3.4.2. FROM: This reviewer (organization, office symbol, and base).
A4.3.4.3. Block 16: As necessary within the reviewer’s organization.
A4.3.4.4. Block 17: Self explanatory.
A4.3.4.5. Block 18: Mark the “approval” or “disapproval” block.
A4.3.4.6. Blocks 19 through 21: Self explanatory.
A4.3.5. The wing IP office’s review.
A4.3.5.1. TO: The SPECAT EMSEC manager (organization, office symbol, and base).
A4.3.5.2. FROM: The wing IP office (organization, office symbol, and base).
A4.3.5.3. Block 16: As necessary within the wing IP office.
A4.3.5.4. Block 17: Self explanatory.
A4.3.5.5. Block 18: Mark the “approval” or “disapproval” block.
A4.3.5.6. Blocks 19 through 21: Self explanatory.
A4.3.6. The SPECAT EMSEC manager’s review.
A4.3.6.1. TO: The SPECAT CTTA (organization, office symbol, and base).
A4.3.6.2. FROM: The SPECAT EMSEC manger (organization and office symbol).
A4.3.6.3. Block 16: As necessary within the SPECAT EMSEC manager’s office.
A4.3.6.4. Block 17: Self explanatory.
A4.3.6.5. Block 18: Mark the “approval” or “disapproval” block.
A4.3.6.6. Blocks 19 through 21: Self explanatory.
A4.3.7. Approval authority: Use this area to approve the temporary waiver.
A4.3.7.1. TO: The requester; organization, office symbol, and base.
A4.3.7.2. FROM: The SPECAT CTTA (organization, office symbol, and base).
A4.3.18.3. Block 28: As necessary.
A4.3.18.4. Block 29: Mark the “approved,” “disapproved,” or “returned for further action” block.
A4.3.18.5. Block 30: The date this form is signed is the date of approval.
A4.3.18.6. Blocks 31 and 32: Self explanatory.